LA IMPORTANCIA DE LA IMPLEMENTACIÓN DE UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI) PARA UNA INSTITUCIÓN DE SEGURIDAD DEL ESTADO

Raúl Enrique Gómez Muñoz
Raul_reg1984@hotmail.com
Universidad Piloto de Colombia
Bogotá, Colombia

Resumen — Para una institución de seguridad del estado es de suma importancia la información que se trata, se almacena y se origina a partir de las diferentes investigaciones, por tal motivo ésta información es altamente sensible por los diferentes operativos y actividades que se realizan a partir de ella, con el fin de propender la seguridad y convivencia ciudadana en el país y por consiguiente si ésta llegase a ser expuesta, extraviada u obtenida de forma fraudulenta podría acarrear situaciones lamentables en las cuales hombres y mujeres podrían perder la vida o poner en riesgo la seguridad y convivencia ciudadana del país, una ciudad o municipio en particular; por tal razón la institución ha tenido la necesidad de implementar un SGSI (sistema de gestión de seguridad de la información), por lo cual se ha analizado los diferentes estándares como COBIT, ITIL e ISO 27001, siendo éste último el tomado por una institución de seguridad del estado para su implementación en la institución, el cual brinda diferentes políticas para el tratamiento y gestión de los riesgos con el fin de lograr un nivel de seguridad de la información óptimo en donde las posibilidades de que se materialice alguna amenaza sea mínima y así preservar de la mejor manera la información institucional.

Abstract — For an institution of state security is important information in question, stored and originates from the various investigations, for this reason this information is highly sensitive for the different operations and activities undertaken from it , in order to move towards security and peaceful coexistence in the country and therefore if it were to be exposed, lost or obtained fraudulently could lead to unfortunate situations in which men and police women could lose their lives or jeopardize the security and citizen of the country, a city or municipality in particular; for this reason the institution has had the need to implement an ISMS (system management security information), which has analyzed the different standards such as COBIT, ITIL and ISO 27001, the latter being the one taken by an institution of state security for deployment in the institution, which provides different policies for the treatment and management of risks in order to achieve a level of security of optimal information where the chances that any threat is minimal materializes and so the best way to preserve institutional information..

Palabras Claves — sistema de gestión de seguridad de la información, seguridad de la información, ITIL, COBIT, ISO27000, análisis de riesgos, integridad, disponibilidad, amenazas, confidencialidad, vulnerabilidad, impacto, consecuencias, evaluación del riesgo, riesgo residual.

I. INTRODUCCIÓN

La información es uno de los activos más apreciados en la institución, ya que ésta es un insumo importante para lograr el objetivo y la misión institucional, por tal motivo con los avances tecnológicos una institución de seguridad del estado ha implementado un gran número de herramientas y aplicaciones con el fin de facilitar las actividades y mejorar la respuesta hacia las peticiones de la ciudadanía, por tal razón se debe asegurar que los canales de comunicación entre los usuarios y éstas herramientas sean seguros, para llegar a éste fin una institución de seguridad del estado ha realizado un estudio de la importancia y ventajas de la implementación de un SGSI (sistema de gestión de seguridad de la información) en la institución entre los siguientes estándares COBIT, ITIL e ISO 27000, después de mencionar éstos estándares analizaremos el por qué la institución decidió implementar el SGSI basado en el estándar ISO 27000 aplicando las sugerencias y referenciándose en la norma **ISO/IEC 27001**, con el cual se quiere lograr la protección y aseguramiento de los procesos, procedimientos y tratamientos que se realicen con la información que posee la institución.

II. METODOLOGÍA

A. MODELOS DE (SGSI) QUE SE PODRÍAN IMPLEMENTAR EN UNA INSTITUCIÓN DE SEGURIDAD DEL ESTADO

A través del tiempo en los momentos de toma de decisiones de impacto para una institución de seguridad del estado una de las variables fundamentales para ésta es el manejo y la información que se posea en ese instante, por tal motivo es uno de los activos de mayor valor para la institución aunque éste no siempre sea tangible, igualmente mediante la implementación del "sistema de gestión de seguridad de la información", busca proteger los activos de la información como insumo fundamental para el cumplimiento de la misión y asegurar la supervivencia de la institución, administrándola y protegiéndola a través de la aplicación efectiva de las mejores prácticas y controles, garantizando la gobernabilidad del país; por lo tanto mencionaremos algunos estándares reconocidos y que pueden brindar las pautas necesarias para su implementación en la institución y cumplir con la necesidad que ésta presenta, así: COBIT, ITIL e ISO 27000.

1. ISO[1]/IEC[2] 27001: La norma adopta una aproximación de proceso al establecimiento, a la implementación, a la operación, el monitoreo, a la revisión, al mantenimiento y a la mejora del sistema de gestión de seguridad de la información de una organización.

La norma plantea un enfoque completo a la seguridad de la información. Los activos de información digital que necesitan protección, documentos en papel, activos físicos (computadoras y redes) y conocimientos de los empleados. Las cuestiones que se tienen que tratar van del desarrollo de competencias del personal a la protección técnica contra los fraudes informáticos.

2. COBIT: (Control Objectives for Information and Related Technology) Es un marco de referencia para la dirección de TI, así como también de herramientas de soporte que permite a la alta dirección reducir la brecha entre las necesidades de control, cuestiones técnicas y los riesgos del negocio. Cobit permite el desarrollo de políticas claras y buenas prácticas para el control de TI en las organizaciones. Cobit enfatiza el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido de TI, facilita su alineación y simplifica la implementación del marco de referencia de Cobit.

3. ITIL: (Information Technology Infrastructure Library) se centra esencialmente en el soporte y en la prestación servicios hacia el cliente.

Sólo contribuye a realizar los objetivos corporativos si el sistema está a disposición de los usuarios y en caso de fallos o modificaciones necesarias, es soportado por los procesos de mantenimiento y operaciones.

Teniendo en cuenta el planteamiento de cada metodología podemos concluir que la norma ISO 27001 es la que se adopta más a las necesidades y requerimientos de la institución por la cantidad de controles que se pueden aplicar con el fin de asegurar una disponibilidad del sistema de forma permanente, preservando la integridad y confidencialidad de los activos de información, del software y hardware que intervienen en su tratamiento como las instalaciones destinadas para su almacenamiento y puestos de trabajo.

[1] ISO: Organización Internacional para la Estandarización

[2] ICE: Comisión Electrotécnica Internacional

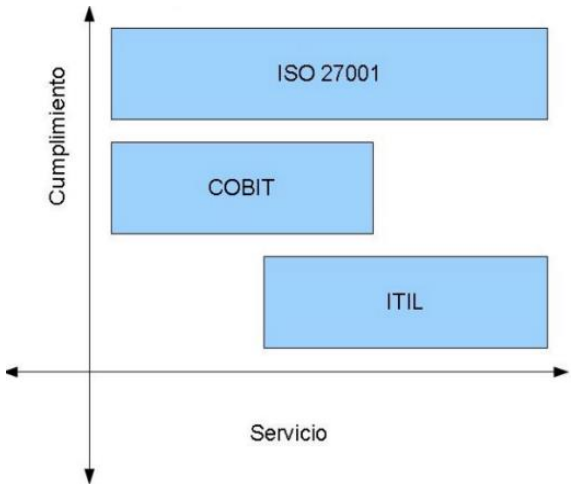

Fig.1 COMPARATIVO DE ESTÁNDARES EN CUMPLIMIENTO Vs SERVICIO
Tomada del sitio web: http://3.bp.blogspot.com/-5X1qq8ic7p8/TjsPEL0ue7I/AAAAAAAAAD0/_OphlGy6nOU/s1600/figura1.jpg

III. IMPLEMENTACIÓN DE UN SGSI PARA UNA INSTITUCIÓN DE SEGURIDAD DEL ESTADO

A. NORMA TÉCNICA NTC-ISO/IEC COLOMBIANA 27001

El área de tecnología de una institución de seguridad del estado fue la encargada de estudiar y evaluar los controles de la norma ISO 27001 que aplicaban a los requerimientos y necesidades institucionales, por tal motivo para formalizar la actividad de implementación del sistema de seguridad de la información ésta área de tecnología creó el manual de seguridad de la información para una institución de seguridad del estado, el cual es importante para la implementación de las políticas de seguridad que son las aplicadas en la institución y los responsables de realizar esta actividad.

Teniendo en cuenta la norma en ISO 27001 tomaremos algunos ítems de la misma los cuales considero que fueron vitales en la creación del manual de seguridad de la información para una institución de seguridad del estado y la implementación del sistema de gestión de seguridad de la información.

B. SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

1. Requisitos Generales

Es importante que la institución establezca, implemente, monitoree, mantenga y realice la mejora continua del SGSI lo cual debe estar debidamente documentado, por lo cual se aplica el ciclo PHVA, que se muestra a continuación.

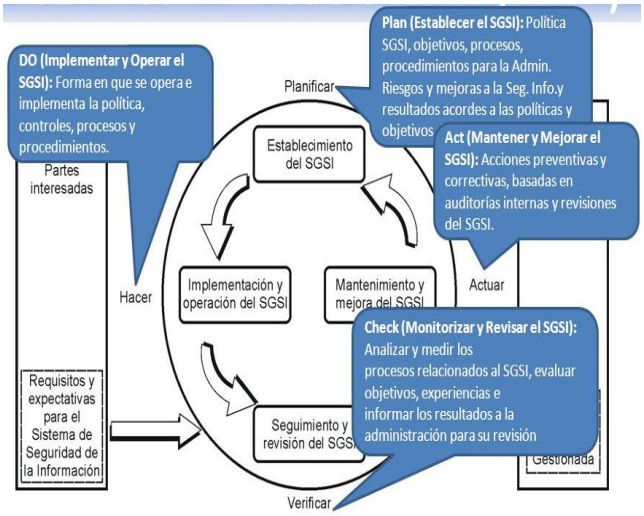

Fig.2 DIAGRAMA Y EXPLICACIÓN DEL CICLO PHVA
Tomada del sitio web:
http://images.slideplayer.es/17/5519241/slides/slide_20.jpg

2. Establecimiento del SGSI

Se debe definir el alcance y límites del SGSI teniendo en cuenta el objetivo, la misión y visión institucional, para posteriormente realizar el análisis y levantamiento de sus activos, una valoración de riesgos de los activos, un plan de tratamiento de los riesgos basándose en las políticas y controles sugeridos en la norma ISO 27001, requisitos legales, niveles de aceptación del riesgo, lo anterior debe estar aprobado mediante la alta dirección de la institución e implementado mediante un acto administrativo.

3. Implementación y operación del SGSI

La institución debe generar un plan de tratamiento de los riesgos planteados según la valoración realizada a los activos, este plan debe ser claro indicando la descripción de los riesgos, controles

a realizar para mitigar los riesgos, responsables del cumplimiento de las actividades, actividad a realizar y del seguimiento del mantenimiento del SGSI, se debe capacitar al personal sobre la importancia y generalidades de la implementación de SGSI, se deben estandarizar los formatos y procedimientos que se encuentran inmersos en los procesos institucionales designados como esenciales para la continuidad y cumplimiento del objetivo, la misión y visión Institucional.

4. Mantenimiento y mejora del SGSI

Se deben realizar actividades de mejora continua del SGSI por lo cual es importante evaluar el sistema y platear las respectivas acciones correctivas y preventivas con el fin de fortalecerlo y llevarlo a una madurez sostenible.

C. RESPONSABILIDAD DE LA DIRECCIÓN

1. Compromiso de la Dirección

La alta dirección de la institución tiene una gran injerencia en la implementación del SGSI, teniendo en cuenta que desde éste nivel es donde se aprueban o no decisiones a nivel de la organización, se disponen los recursos para la implementación y mantenimiento del sistema, se toma la decisión del nivel de aceptación de los riesgos.

2. Provisión de recurso

Éste ítem es importante para la implementación del SGSI ya que de él depende los recursos para poder implementar, operar, revisar y mantener el sistema, aparte de esto se debe tener en cuenta la capacitación al personal en general sobre la importancia del sistema e igualmente al personal técnico específico que liderará y orientará a la alta dirección sobre las actividades que se deben seguir e implementar para el mantenimiento y madurez del SGSI.

D. AUDITORIAS INTERNAS DEL SGSI

Las auditorías internas son de gran importancia para determinar el cumplimiento de los objetivos, los controles y los procedimientos de cada proceso. Se deben realizar un plan de auditorías el cual indique lo siguiente: cronograma de auditorías, procesos que van a ser auditados, responsables de la auditoria (auditores los cuales no deben auditar su trabajo); es responsabilidad del comandante o director de la unidad auditada el realizar las actividades y toma de decisiones necesarias para dar cumplimiento a las oportunidades de mejora y la subsanación de las no conformidades encontradas durante la auditoría realizada.

E. MEJORA DEL SGSI

1. Mejora Continua

Ésta etapa del proceso nos sirve para mejorar y madurar el SGSI y está compuesta por las siguientes acciones: Preventiva y correctiva las cuales nos dan las pautas para mejorar falencias del sistema y/o eliminar no conformidades encontradas durante una auditoria, identificando las causas de su no cumplimiento y planteando planes de trabajo con sus respectivas actividades con el fin de subsanar las tareas que no se estaban cumpliendo, tener en cuenta el ciclo PHVA.

Como resumen de los temas a tener en cuenta para la implementación del sistema de gestión de seguridad de la información tenemos la siguiente gráfica:

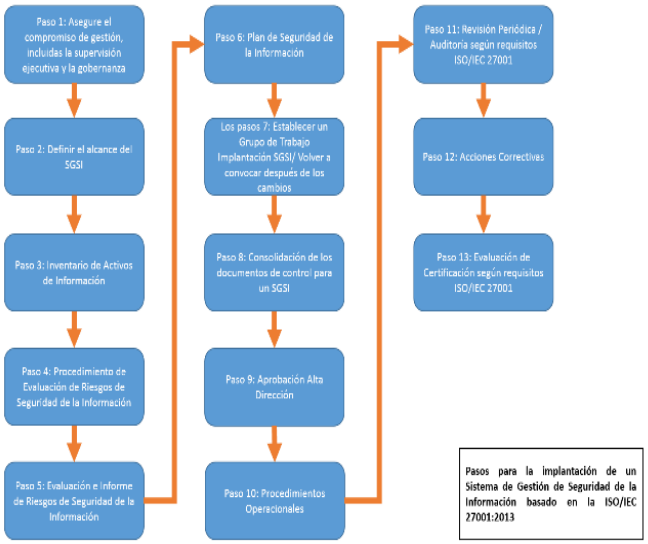

Fig.3 PASOS PARA LA IMPLEMENTACIÓN DE UN SGSI BASADO EN ISO/IEC 27001

Tomada del sitio web:
http://iticsec.com/portal/images/pasos%20sgsi.png

F. CONTROLES QUE SE DEBERÍAN APLICAR

En éste ítem hablaremos del control general para cada actividad por lo cual no profundizaremos en los controles específicos que componen cada control general.

1. POLÍTICAS DE LA SEGURIDAD DE LA INFORMACIÓN

La función de este control está orientado a la orientación y apoyo que debe ser brindado por parte de la dirección, para la implementación del sistema de gestión de seguridad de la información (SGSI) de acuerdo con los requisitos del negocio, con las leyes y los reglamentos vigentes.

2. ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

Mediante la aplicación de éste control se establece el marco de referencia de la gestión con el fin de controlar la implementación y operacionalización del SGSI dentro de la organización asignando roles, responsabilidades, realizar la estructura orgánica de la organización con el fin de separar áreas y dependencias según su funcionalidad en la misma, se debe realizar los acercamientos correspondientes con las autoridades locales en caso de ser requerido por algún incidente.

3. DISPOSITIVOS MÓVILES Y TELETRABAJO

Dicho control es vital para la organización teniendo en cuenta el gran uso de dichos dispositivos, por lo cual éstos sistemas deben ser administrados y controlados desde el nivel central bloqueando la facultad de instalación de software o aplicaciones que pongan en riesgo la información institucional, igualmente se les debe realizar revistas físicas con el fin de verificar su integridad y el uso que le están aplicando.

4. SEGURIDAD DE LOS RECURSOS HUMANOS

Se debe verificar en el proceso de incorporación las capacidades y requisitos profesionales que debe tener el personal al momento de ser vinculado a la organización, cuando es un funcionario activo en la institución éste debe conocer sus responsabilidades y compromisos con la seguridad de la información, algo muy importante a tener en cuenta en el proceso de talento humano es el procedimiento de terminación de contrato y eliminación de usuarios.

5. GESTIÓN DE ACTIVOS

Se deben identificar los activos de la organización definiendo las responsabilidades del personal sobre los activos que tienen asignados con las protecciones y cuidados que deben tener sobre los mismos, se debe capacitar al personal e incluir el uso de cláusulas de confidencialidad de la información en las cuales se estipule la no divulgación, la no modificación, el retiro o eliminación de la información almacenada en los equipos sin previa autorización.

6. CONTROL DE ACCESO

Este control lo debemos implementar tanto a nivel físico como a nivel de software y de aplicaciones de la siguiente manera:

a. nivel físico: debemos implementar los dispositivos necesarios para impedir el acceso a las diferentes áreas de la organización y más aún a los lugares en donde se encuentra almacenada o es tratada la información, ejemplo (funcionarios de seguridad, puertas con sus respectivas políticas de acceso, bitácoras o registros de ingresos del personal y demás que estime pertinente la organización).

b. El control de acceso a software y aplicaciones: va asociado a la creación de usuarios con los roles necesarios para realizar sus actividades laborales, cabe anotar que los usuarios deben utilizar un password con unas características que lo hagan difícil de resolver o mediante la implementación de factores de autenticación que puede ser de 2do o 3er factor (ejemplo los factores de autenticación pueden ser los siguientes: algo que se tiene "token", algo que se sabe "password", algo que se es "biometría").

7. CRIPTOGRAFÍA

Se debe implementar un sistema criptográfico con el fin de darle un mayor nivel de protección a la

información, el cual se pueda utilizar entre otras cosas para: cifrar dispositivos móviles, generar llaves para enviar y recibir comunicados, realizar la firma digital para los diferentes procedimientos que se realicen en la institución.

8. SEGURIDAD FÍSICA Y DEL ENTORNO

Éste control se debe aplicar de forma muy consciente ya que se compone de una parte tecnológica y otra Humana en donde participa activamente el personal de seguridad de instalaciones e igualmente los funcionarios de la institución que deben velar porque no se encuentre personal ajeno a las dependencias deambulando por las mismas sin previo acompañamiento de algún funcionario.

Por otra parte mediante este control se debe prevenir la pérdida, daño o robo de los activos de la institución lo cual puede afectar algún proceso, procedimiento o actividad de la dependencia a la cual pertenecía el activo.

9. SEGURIDAD DE LAS OPERACIONES

Para la aplicación de este control se deben tener en cuenta varias actividades, así:

a. Se debe documentar cualquier actividad que se realice en el sistema, como lo son: actualización de parches, apagados de mantenimiento, copias de respaldo, manejo de los medios de almacenamiento, se debe implementar un ambiente de desarrollo de software con el fin de verificar y hacer las pruebas necesarios de los productos antes de ponerlos en producción y exponer el sistema a una posible vulnerabilidad de seguridad.

b. Se debe realizar campañas de concienciación al personal sobre los riesgos que se pueden tener al instalar programas de dudosa procedencia los cuales pueden contener código malicioso y afectar los sistemas de la organización, por otra parte se debe contar con una plataforma tecnológica que realice la detección, prevención y recuperación del sistema en caso de alguna anomalía presentada por un código malicioso (IPS, IDS y Firewall).

c. Se deben realizar copias de respaldo de la información, del software e imágenes de los sistemas de manera periódica e igualmente realizar las respectivas pruebas del funcionamiento de dichos respaldos con el fin de verificar su funcionalidad.

d. Se debe llevar un registro de los usuarios que tienen acceso al sistema, eventos presentados en el sistema, logs de auditoria, actualizaciones del sistema, direccionamiento de red, eventos relacionados con el antivirus y sistemas de detección de intrusos.

e. Se debe tener un protocolo para la realización de actualizaciones de sistemas operativos, aplicaciones y programas de los equipos de cómputo.

f. Se debe verificar las vulnerabilidades técnicas que posee un sistema con el fin de verificar el nivel de criticidad del mismo y así analizar las formas de solucionar o proteger dichas vulnerabilidades para así poder implementar el sistema o no.

g. Se debe coordinar en las actividades de auditoria los horarios y alcances de la misma en relación con los sistemas con el fin de no generar interrupciones de los mismos, se debe prever los permisos de acceso para la auditoria el cual debe ser de solo lectura, en caso que se requiera de hacer pruebas que afecten el funcionamiento normal del sistema estas se deberían realizar en horarios no laborales.

10. SEGURIDAD DE LAS COMUNICACIONES

Para la implementación de éste control se deben tener en cuenta las siguientes actividades:

a. Gestión de los equipos en dominio de la organización con el fin de llevar un control del uso de los recursos de red y realizar el despliegue de las políticas de seguridad y actualización de antivirus.

b. Se deben configurar Vlan para separar los procesos de la organización con el fin de brindar mayor seguridad, rendimiento de recursos e integridad de la red.

c. La información institucional debe ser transmitida únicamente mediante el uso de los correos de la organización con el fin de prevenir fugas de información, igualmente se debe prohibir el uso de almacenamiento en la nube y enviar la información únicamente por los medios autorizados y controlados de la institución.

11. RELACIONES CON LOS PROVEEDORES

Éste control debe ser tratado adecuadamente teniendo en cuenta que es personal ajeno a la institución y por ende no conocen las políticas de seguridad de la información de la misma, por tal razón se aconseja realizar las siguientes actividades entre otras que puede aplicar cada unidad de la institución según su criterio:

a. Definir los tipos de acceso que se le va a conceder a los proveedores y que controles se les va a realizar a los mismos.

b. Capacitar y concienciar al personal de proveedores sobre las políticas de seguridad de la información, cuando estos tengan acceso a la información o realicen alguna actividad con la misma.

c. El personal de proveedores según el acceso a la información debe pasar por un estudio de seguridad.

d. Todo el personal de proveedores debe diligenciar los formatos estipulados de confidencialidad de la información y tratamiento a la misma.

e. Se deben manejar cláusulas contractuales con el fin de asegurar el cumplimiento del contrato y la confidencialidad de la información que pertenece a la organización.

IV. CONCLUSIONES

Se analizó y estudio que metodología se iba a utilizar como referencia para la implementación del SGSI, teniendo en cuenta las características de la organización como lo son: actividad económica, objetivo de la institución, tamaño de la institución, recursos disponibles para la implementación.

Una institución de seguridad del estado decidió implementar el sistema de gestión de seguridad de la información basada en la norma técnica ISO 27001.

Se identificó el apoyo por parte de la alta dirección el proyecto de implementación del sistema de gestión de seguridad de la información (SGSI).

Para la implementación y cumplimiento del sistema de gestión de seguridad de la información, una institución de seguridad del estado mediante un acto administrativo formal el cual entro en vigencia desde su publicación en donde se “adopta el manual del sistema de gestión de seguridad de la información para la institución”, el cual fue realizado tomando como referencia la norma ISO 27001-27002.

Por ser una institución tan grande se ha ido realizando el seguimiento y proceso de implementación del SGSI por unidades iniciando por las diferentes direcciones que la componen y las unidades desconcentradas a nivel nacional se ha realizado la aplicación de algunos ítems del manual de seguridad de la información según su aplicabilidad y funcionalidad de cada unidad.

Se capacitó al personal responsable de TI de cada unidad desconcentrada con el fin que éstos realicen funciones de promotores de seguridad de la información para realizar capacitaciones al personal de sus unidades con el fin de generar conciencia sobre la importancia de la información y las diferentes acciones que ponen en riesgo los activos de información e igualmente las actividades que se deben hacer para mitigar estos riesgos.

V. REFERENCIAS

1. http://www.pmg-ssi.com/2016/01/norma-iso-27001-vulnerabilidad-sistema/

2. http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

3. http://itil.osiatis.es/Curso_ITIL/Gestion_Servicios_TI/fundamentos_de_la_gestion_TI/que_es_ITIL/que_es_ITIL.php

4. http://www.isaca.org/COBIT/Pages/COBIT-5-spanish.aspx

5. http://seguridadinformacioncolombia.blogspot.com.co/2010/07/que-es-cobit.html

6. http://www.dnvba.com/cl/certificacion/sistemas-de-gestion/Seguridad-de-la-Informacion/Pages/ISO-27001.aspx

7. NORMA TÉCNICA COLOMBIANA NTC-ISO-IEC 27002:2013 (Primera actualización)

8. https://securingthehuman.sans.org/newsletters/ouch/issues/OUCH-201211_sp.pdf

9. http://iticsec.com/portal/